Správa a dohled privilegovaných účtů

DATA SYS

spolehlivě · nejvýhodněji

AGENDA

QUICK WIN
VIDEO LOGY

THYCOTIC
A WALLIX

DATASYS
KOMPETENCE

ŘÍZENÍ
PŘÍSTUPŮ A ÚČTŮ

STUDIE
PŘÍPADOVÉ

Požadavky zákona o kybernetické bezpečnosti: §22

§22 – Zaznamenávání konkrétních typů činností

1. přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,
2. **činností provedených administrátory,**
3. **úspěšné i neúspěšné manipulace s účty, oprávněními a právy,**
4. neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,
5. činností uživatelů, které mohou mít vliv na bezpečnost systému,
6. zahájení a ukončení činností technických aktiv,
7. kritických i chybových hlášení technických aktiv a
8. **přístupů k záznamům o událostech a pokusy o manipulaci se záznamy**

Top 10 Security Projects for 2019

1 Privileged Access Management

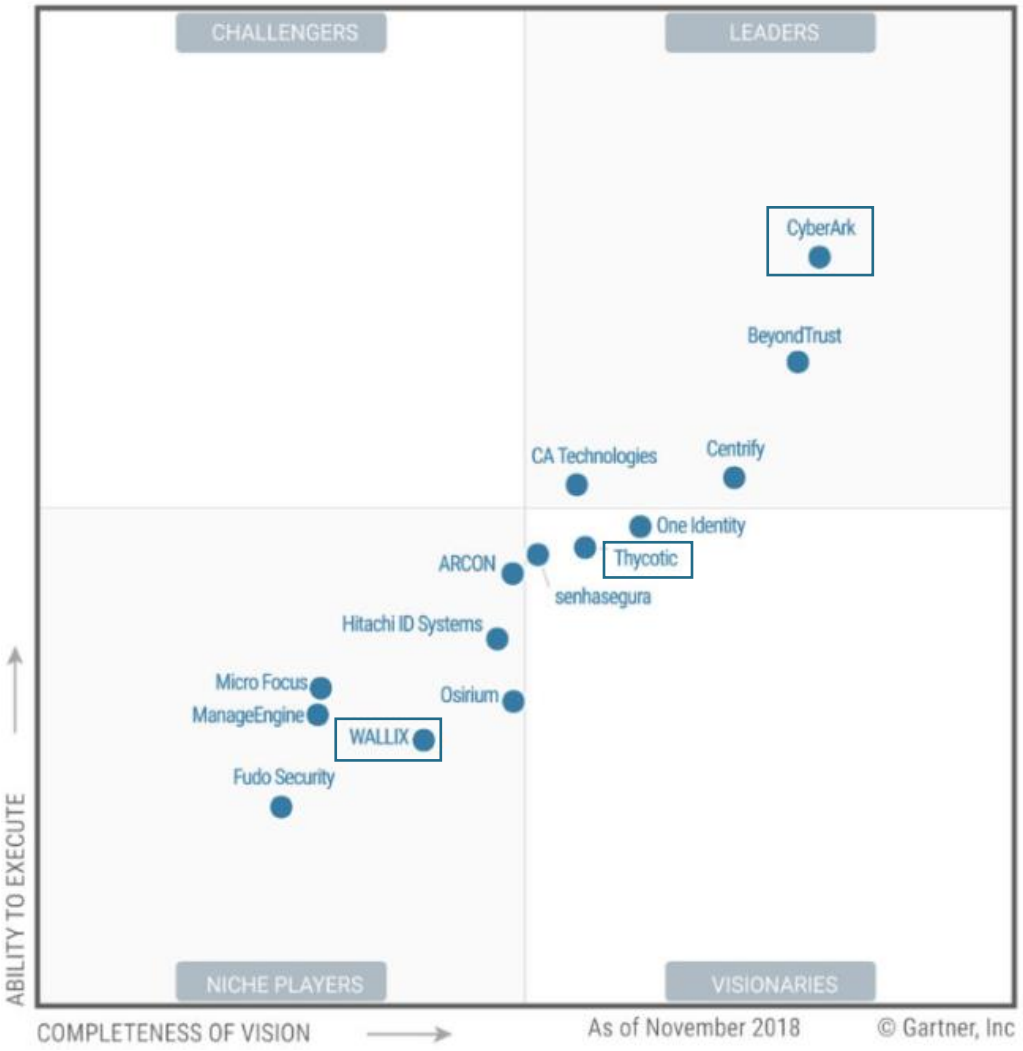
Top Tips

- PAM projects should at least support multifactor authentication (MFA) for all administrators.
- PAM for third-party access should be a priority.

6 Bu Co

Top Tips

- Look to y to provid integrati training



DATA SYS

privilegované
přístupy dodavatelů
>>> **video logy**

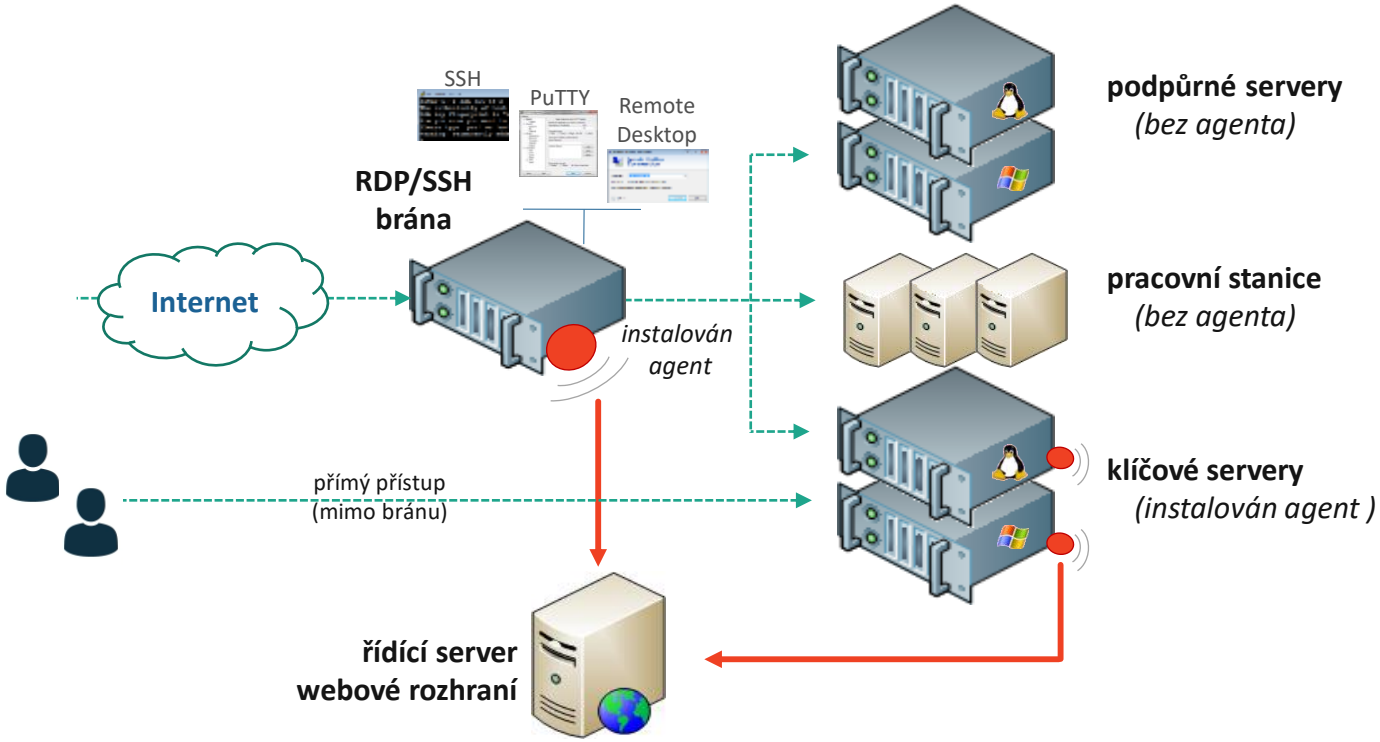
Vědět je fajn, ale co je lepšího, než vše VIDĚT?

Řízení přístupů privilegovanými účty

- Video logy uživatelských relací
- Indexované snímky obrazovek
- Podpora doplňkové autentizace
- Chráněný běh agenta

OBVYKLÝ PRINCIP NASAZENÍ

Nahrávání na „jump“ serveru a na klíčových serverech.



DALŠÍ BENEFITY

Jeden z mála bezpečnostních nástrojů se zřetelným ROI

- Optimalizace servisních smluv

observe it EKRAN QUICK WIN

- Přenos znalostí na juniorní správce
- Automaticky vznikající provozní deník
- Snazší budování zástupnosti v týmu

DATA SYS

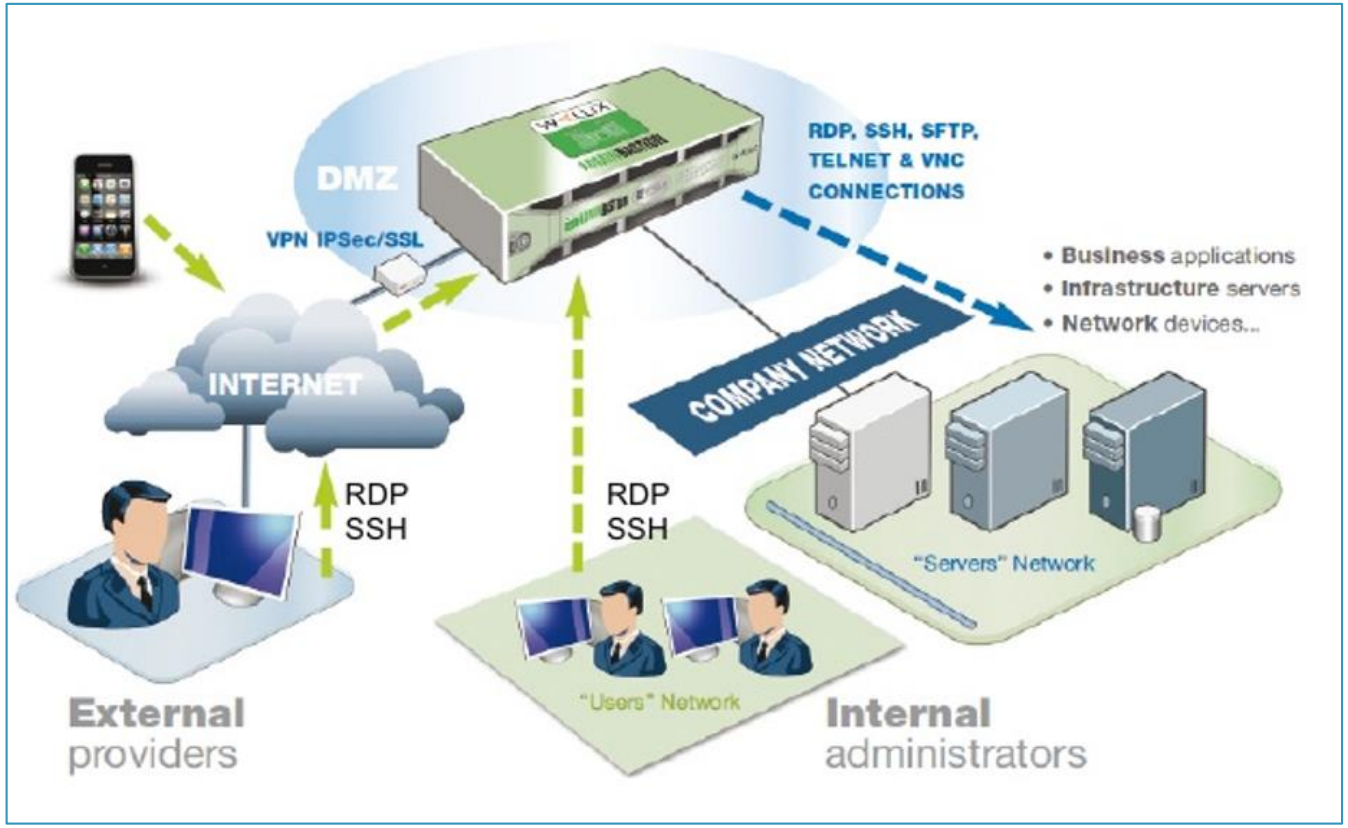
kontrola / řízení

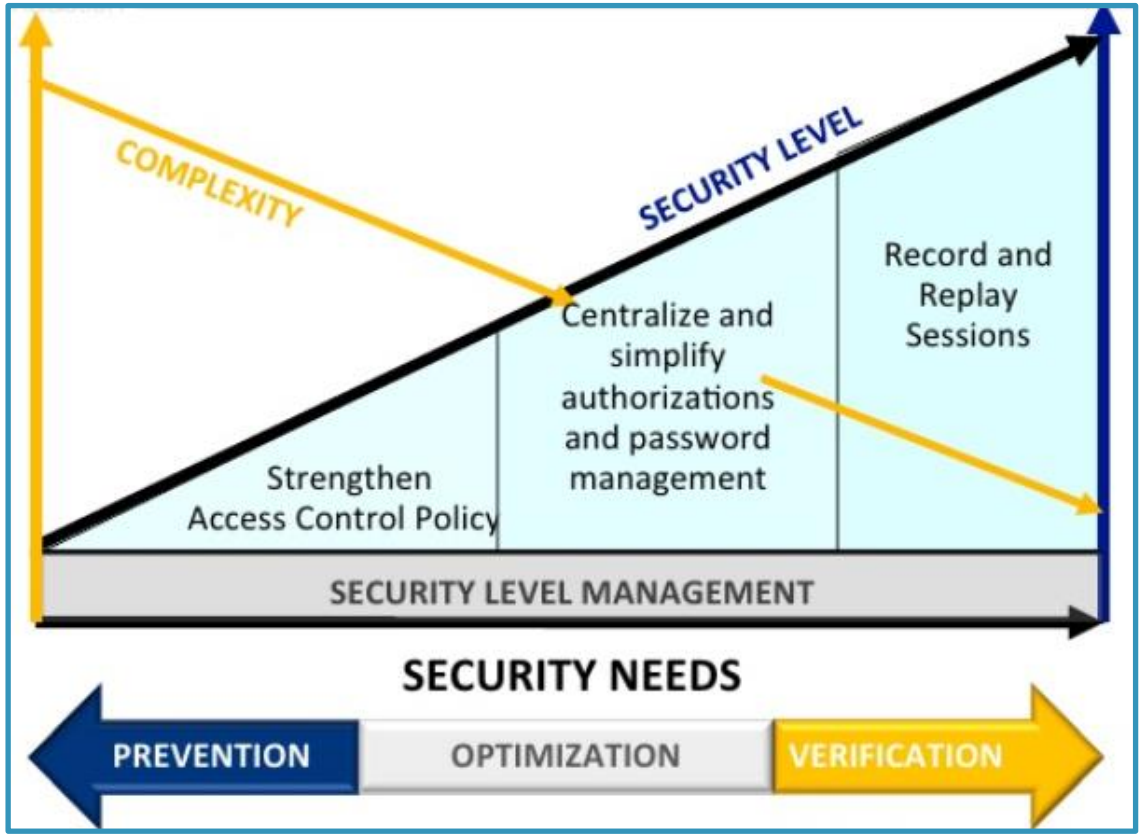
privilegovaných

přístupů a účtů

ŘÍZENÍ PŘÍSTUPŮ

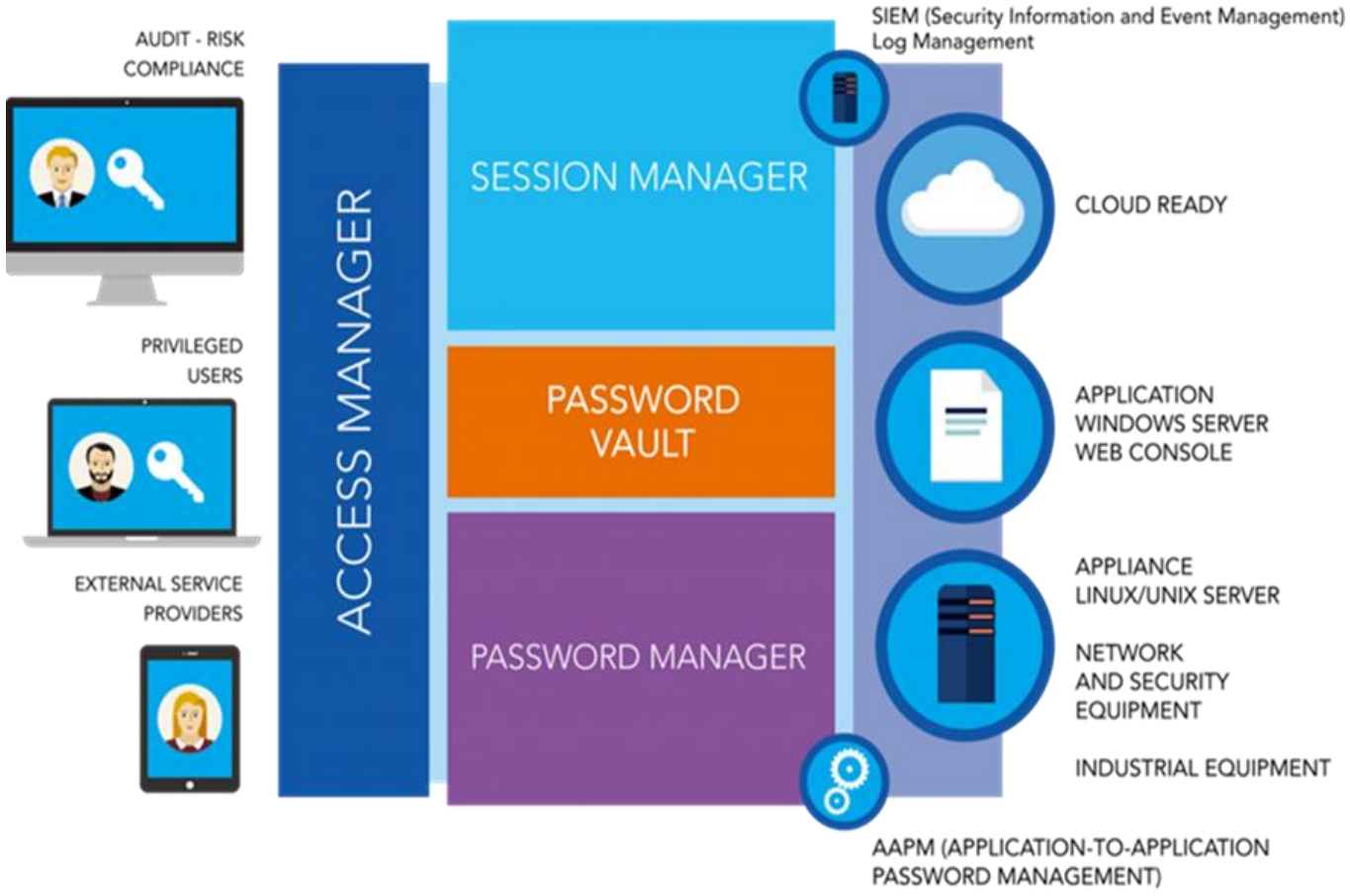
Přístupová brána mění zažité postupy = vyšší komplexita





ARCHITEKTURA

- Zabezpečený trezor hesel
- Pravidelná obměna hesel
- Řízení přístupových relací
- Nahrávání relací



RÁMCOVÉ SROVNÁNÍ

Nástroje pro řízení privilegovaných relací	CyberArc Privileged Session Manager	Thycotic Secret Server (Session Monitoring)	WALLIX Bastion (Session Manager)
Forma dodání nástroje	„hardened“ windows server	standardní windows server	„hardened“ (linux) appliance
Architektura nástroje	funguje jako vzdálená plocha s možností transparentního SSH	přístupový portál s „launchery“ napřímo nebo skrz SSH proxy	přístupový portál s možností transparentního režimu
Možnosti restrikcí	s restrikcemi na spouštění konkrétních aplikací	s restrikcemi na spouštění konkrétních aplikací (klientů)	s restrikcemi v rámci protokolů nebo na spouštění aplikací
Možnosti řízení hesel	sdílení a řízení hesel servisních účtů je základní funkcionalitou	sdílení a řízení hesel servisních účtů je základní funkcionalitou	zahrnuje modul pro řízení hesel – a podporuje i externím
Podoba nahrávek	session logy s doprovodnými video soubory	video logy s „timeline“ aktivit	indexované video logy

- **Silný password mgmt**
- **Kvalitní session mgmt**

- **Silný session mgmt**
- **Slabší password mgmt**

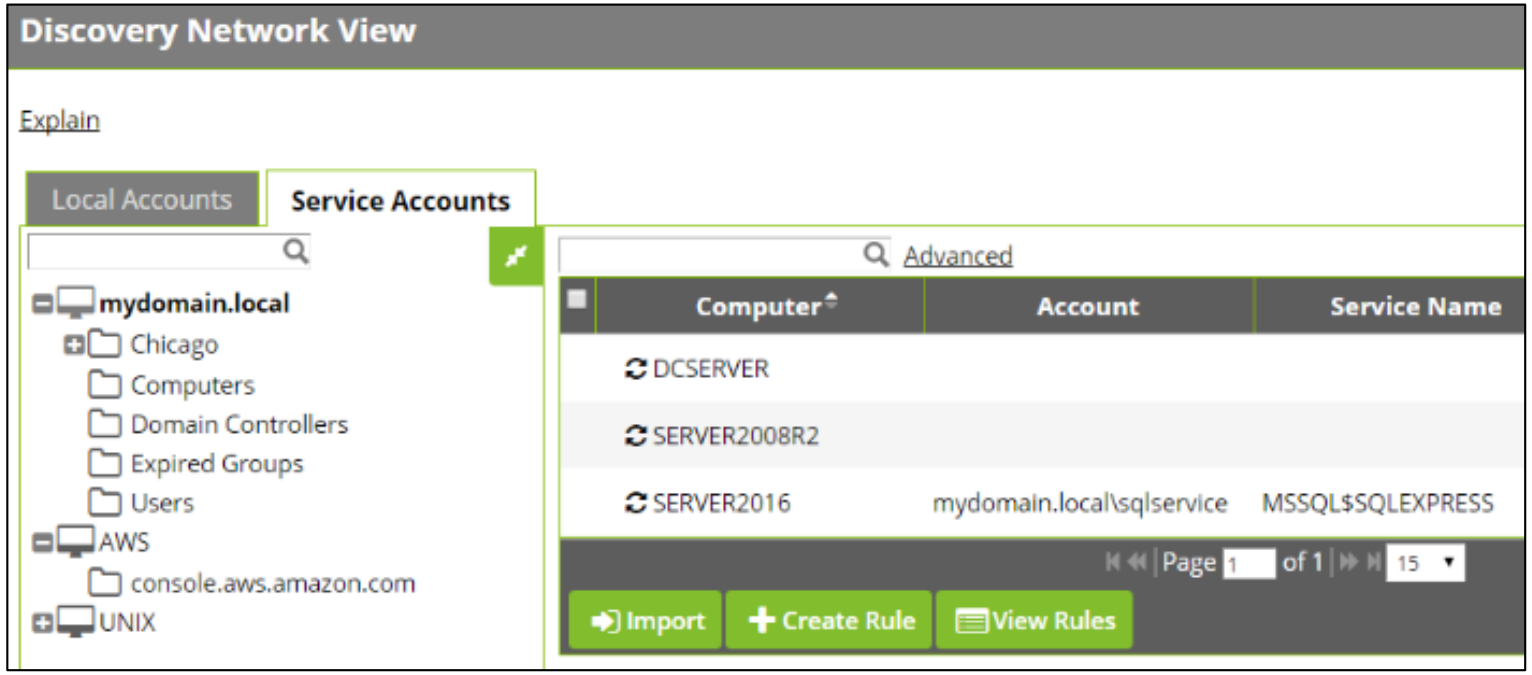
DATA SYS

nástroj **Thycotic Secret Server**

Thycotic Secret Server – vše se točí kolem „secrets“

Webový portál pro bezpečné sdílení a řízení hesel k servisním účtům
Poskytuje prostor i pro bezpečné uložení osobních hesel a klíčů

- Rozkrytí účtů
- **Rozkrytí závislostí**
- Převzetí kontroly
- Vynucení politik hesel



Poskytuje automatizaci správy hesel

- Automatizace pravidelných změn hesla
- Knihovna *pluginů* pro správu systémů
- Podpora přístupu prostřednictvím SSH klíčů
- Podpora obměny SSH klíčů na serverech

- Active Directory Account
- Blue Coat Account
- Blue Coat Enable Password
- Cisco Account
- Cisco Enable Secret
- ESX/ESXi (API)
- F5 BIG-IP Root Account
- Generic ODBC DataSource
- HP iLO Account
- Juniper Account
- MySQL Account
- Office365
- Oracle Account
- PostgreSQL Account
- SQL Server Account

...

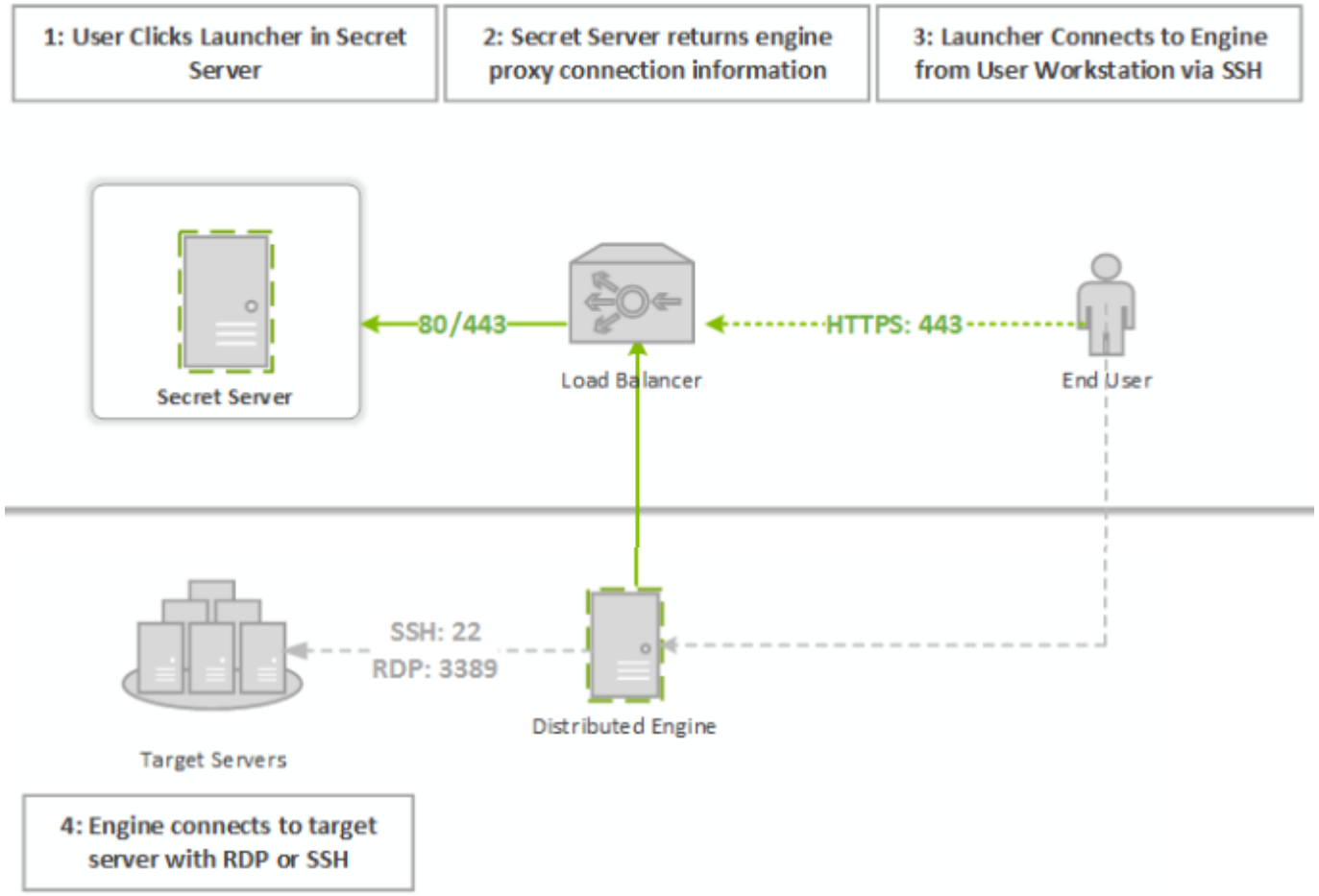
Přístup do databáze s nastavením dočasného hesla

thycotic

Privilegovaný přístup „delegací“ může fungovat takto:

1. **Uživatel** se přihlásí k webovému portálu svým účtem.
2. **Nástroj** uživateli nabídne oprávněné systémy a jim příslušné privilegované účty.
3. **Uživatel** zvolí účet a zažádá o schválení přístupu ke konkrétnímu privilegovanému účtu.
4. **Supervizor** je notifikován o provedené žádosti a provede ve webovém portálu schválení.
5. **Uživatel** je notifikován o schválení a zažádá si v portálu o propůjčení přístupového hesla.
6. **Nástroj** změní heslo daného privilegovaného účtu a zobrazí jej uživateli.
7. **Uživatel** vykoná s využitím jen jemu známých přihlašovacích údajů potřebné aktivity.
8. **Uživatel** ve webovém portálu ukončí zápůjčku přístupového hesla.
9. **Nástroj** změní heslo daného účtu, aby jeho znalostí už nikdo nedisponoval až do další zápůjčky.

Thycotic Secret Server – připojení přes proxy engine



1. **Uživatel** ve webovém portálu klikne na „Launcher“
2. **Nástroj** poskytne „spouštěči“ informaci potřebnou pro připojení přes proxy (distribuovanou).
3. **Klientský program** (spouštěč) se z uživatelova PC připojuje skrz SSH proxy.
4. **Distribuovaná proxy** se připojuje na koncové zařízení protokoly RDP nebo SSH.

Vzdálená plocha při integraci s Active Directory

Integrovaná autorizace

- Ověření členství v AD skupinách
- Mapování na PAM role

Připojení na koncový systém

- Již bez zadávání hesla
- Různými síťovými protokoly

Přihlášení uživatele

- K portálu nástroje
- Účtem v AD

Nabídka připojení

- Dle přiřazených rolí
- Na konkrétní servery a účty

Kontrolovaná relace

- Nahrávání s metadaty
- Protokolová omezení

DATA SYS

modelové situace a **případové studie**

Česká pošta s.p.

- ❑ Nahrávání administrátorských relací pro 1000+ monitorovaných serverů
- ❑ Linux (CentOS/RHEL, Debian/Ubuntu, SLES), SPARC Solaris, Windows
- ❑ Integrace se SIEM

- ✓ Implementace během dvou měsíců
- ✓ Doprogramování podpory pro SPARC Solaris zóny výrobcem
- ✓ Předávání detekovaných alarmů i všech záznamů o relacích (syslog/CEF)

Skupina AGEL – desítky nemocnic a jiných zdr. zařízení

- ❑ Potřeba centrální instalace s výraznou autonomií správy organizacemi
- ❑ V první fázi desítky, do 6 měsíců stovky Windows a několik Linux serverů

- ✓ Multi-tenantní instalace, centrální bezpečnostní dohled
- ✓ Množstevní sleva odpovídající cílovému počtu monitorovaných serverů

DATA SYS

integrátor
pečlivě volených
špičkových
technologií

SOUHRN - PROČ PASM?

- Potřebujete utáhnout zabezpečení a zajistit soulad s normami?
  - ➢ **Máme nástroje, je to jednoduché!**
- Získejte přehled o práci dodavatelů a ušetříte náklady!
  - ➢ **Co je lepšího, než vše vidět!**
- Potřebujete zlepšit zastupitelnost administrátorů?
  - ➢ **Učte se průběžně i zpětně!**

PROČ S NÁMI? MÁME ZKUŠENOSTI, ZNÁME NÁSTROJE.

Kontrola privilegovaných přístupů

Video logy relací

observe it

EKRAN

Řízení privilegovaných přístupů

Kam se kdo může připojit

thycotic

WALLIX
TRACE, AUDIT & TRUST

Správa přístupových hesel

Chráněné úložiště hesel

REFERENCE - PASM

Česká pošta

1000+

Ministerstvo spravedlnosti České republiky MS ČR

OKIN

Letos:

Zlínský kraj

Česká televize

Vodárna Plzeň

GECO

artesa

Lagardère TRAVEL RETAIL

Mero MERO ČR, a.s.

AGEL

DATA SYS

Pojďme na to!

Jednodušší už to nebude